Office of Information Technology Services

Service Level Agreement for Hosting Services

Contents

1 Executive Summary

Hosting Services provides the servers and support resources to allow an agency to run business applications and systems through a reliable, monitored, secure and managed IT server solution. The hosting services solution also includes agencies file, print and directory service support which provides the agency the ability to log into the network and share data and resources. This support is available to all agencies that have a local area network (LAN) consisting of communication products linked together with state standard wiring, switches, and network operating systems.

2 Service Provided, Availability and Support

2.1 Service Objective

This Service Level Agreement (SLA) documents Hosting Services provided by ITS Computing Services for an agency. The ultimate objective of this Agreement is to document the support and processes necessary to ensure high-quality and timely delivery of this service. This document clarifies all parties' responsibilities and procedures to ensure Customer needs are met in a timely manner. Although the SLA is in the form of a document that defines a level of service, the desired outcome is to provide a clear understanding and expectation of the service ITS provides and to work with the Customer as a business partner to improve and optimize the business as well as improve ITS services.

2.2 Service

The scope of services is all hosted server equipment and network operating system software, to support the Sun, Linux, UNIX, Windows, Novell Netware and Microsoft Active Directory environments. This includes the support of the technical environment, the performance of activities required to ensure the service remains secure, reliable and operational, and the performance of activities necessary to implement the above environments.

- Service capability includes:
  - Managed server environment including hardware, software, environment (ITS and DOA building datacenters only) and resources

- Compliance with statewide IT policies and standards
- Ownership of the entire infrastructure lifecycle (ITS and DOA building datacenters only)
- Predictable monthly cost

- Service components include:
  - Server computing hardware and periodic refreshes of equipment
  - Infrastructure components including associated replacements and spares
  - Server operating system software
  - Conditioned electrical power, raised floor space and environmental conditioning unless server is required (due to network limitations or data resiliency) to be located outside of the ITS Data Center or DOA Building Data Center
  - Provide UPS, proper power requirements and environmental conditioning requirements for areas outside of the ITS Data Center or DOA Building Data Center
  - Backup and recovery of data, this is further defined in Appendix B
  - Vaulting and retention of data backup tapes (ITS Datacenter only)
  - Use of hardware and/or performance monitor software to monitor the server including disk space, memory and CPU utilization

- Service implementation and support includes:
  - Consultation regarding server options and configurations
  - All required activities to complete service installation and on-going support of hardware, OS software and utility support software
  - Coordinate all necessary (vendor recommended or security mandated) OS service and security patches that need to be installed during ITS standard maintenance windows
  - Coordinate change management with Service Level Management to Customer Change Management contacts, including negotiation to determine times required for outages that result in any impact to Customer operations
  - When a problem is diagnosed or there are trends indicating a problem, the ITS technicians and ITS CSC will coordinate the communication to the customers. The ITS technicians will manage the service call (call out the vendor to service the equipment) to the hardware, software or storage vendors through successful resolution of the problem.
  - Service includes use of performance monitor software for monitoring of server environment, including disk space, memory and CPU utilization. ITS will work with the customer to define further requirements needed to performance monitoring including applications. ITS will also work with customer to determine how the customer can receive monitoring reports and alerts.
  - When required, ITS will support the customer with physical access to the server environment by visiting the site where the server is located for the purpose of problem resolution. This means hands-on with the server and a Computing Services technician will work with the customer to gain access to the room and equipment.
  - ITS can provide remote support via VPN to the Customer for their application support activities for an additional charge. Customer uses standard software such as remote desktop and terminal services will be able to use remote support at no additional charge. There may be instances where VPN may be required for certain levels of access. This will be determined between the customer and ITS.
  - Access to server and OS components will be tiered based on application and database needs and will be granted in a secure manner that is in compliance with statewide and internal security policies, procedures and Information Security Office standards
  - Support of network operating system account creation, password management and security rights management (server based only)
  - Support 24x7x365 via the Customer Support Center for problems or service requests

using the iWise system to log and track all incident and request tickets

- Business direction and strategy includes:
  - Work with Customer to determine disaster recovery needs for each application residing on a hosted server
  - Work with Customer by assisting in local and statewide planning and assist in the evaluation and planning of new and existing systems
  - Facilitate annual service review meeting with the Customer

2.3 Services Out of Scope

- The management of applications and application services will not be the responsibility of Hosting Services but is expected to be handled by the agency.
- The management of database and database services will not be the responsibility of Hosting Services but is expected to be handled by the agency. Database services are offered by ITS and if selected as a service from ITS then ITS will be responsible for database services.
- Monitoring of applications will partially be handled by the monitoring of disk space, memory and CPU usage using hardware and/or performance monitor software. If additional monitoring is needed such as services or processes within a server then the agency application team will develop the appropriate scripts or work with ITS to determine if hardware and/or performance monitor software can monitor the application services.
- ITS will not be responsible for Internet network components and network components terminating at facilities outside of the ITS's sphere of control.
- ITS will not be responsible for software and hardware not specified in the description of components hosted by ITS. This list is in Appendix A.
- ITS will not be responsible for administrative support of account creation, group creation, rights assignments, application installation and password administration as they apply to business applications.
- ITS will not be responsible for administrative support of account creation, group creation, rights assignments, database installation and password administration as they apply to database systems.

2.4 Hours of Availability

The service described in this SLA is available from 24 hours, 7 days a week, 365 days a year. Exceptions are noted below.

Time Frame	Description
Weekdays	• Hosting Services will have a scheduled maintenance window during normal weekday operations on Thursday from 4:00AM to 6:00AM for network maintenance.
Weekends	• Hosting Services will have a scheduled maintenance window on Sundays from 4:00 a.m. to 12:00 noon for routine maintenance.
Holidays	• There will be no Hosting Services scheduled outages during normal weekday holiday operation.
Non Routine	An emergency change is an event in response to an incident that requires immediate attention. This event is to correct a broken or failing service, or to implement quickly, preventative

	maintenance. To proceed: • Contact your manager • Your manager is responsible for escalation • Contact the Customer Support Center • Build and implement the Change • Contact the Customer Support Center when complete • Complete a Post Implementation Review Non routine maintenance windows, other than emergencies, will be processed via the SLA change request process.

2.5 Hours of Support

The support service described in this SLA is available from 7*:00 a.m. to 6:00 p.m*. *Monday through Friday* eastern time (except on State holidays).

Staff support is provided during Non-Business Hours by a scheduled ONCALL rotation. Emergency support is available after normal Business Hours

2.6 Constraints on Availability

Scheduled Maintenance Windows:
All activities will be conducted within the customer maintenance window unless other arrangements are made.

Emergency Maintenance Windows:
Emergency Maintenance windows will be handled through the urgent change process.

2.7 Contacting Support

Call the Customer Support Center (CSC) at **919-754-6000** or toll free at **1-800-722-3946.**
-or –
Email the CSC at ITS.Incidents@ncmail.net

2.8 Customer Support Center Response Times

The following priority chart shows response time after initial Assessment/Assignment, creation of iWise ticket by the Customer Support Center, and acknowledgement of the ticket to the customer, including the provision of a ticket number. Times are measured in clock hours and/or minutes unless otherwise specified. If a ticket is initiated by a telephone call, it will be created within 10 minutes; if initiated by email, the ticket will be processed within 30 minutes.

Target Incident Response Time:
The time the Second Level support has to begin to actively work a ticket.

Target Status Update Time:
The time interval the assigned group / ticket owner has to update the ticket.

Target Customer Notification Time
The interval that the Customer Support Center has to update the customer on ticket status.

Target Resolution Time:

The total time from ticket creation to resolve the incident and restore service to the user.

Target Percentage of Calls Resolved on Time:

The percentage of calls that meet the priority time frame criteria.

2.9 Priority Chart

Priority	Target Incident Response Acknowledge-ment Time	Target Status Update Interval	Customer Status Update Interval	Target Resolution Time	Target % of Calls Resolved on Time
1	15 minutes	Every 15 minutes	CSC will update every 30min	4 clock hours or less	90% rising to 95% within first 6 months of rollout; Reassess target at end of 6 months
2	30 minutes	Within 1 hour then every hour thereafter	CSC will update every 2 hours	8 clock hours or less	90% rising to 95% within first 6 months of rollout; Reassess target at end of 6 months
3	2 hours	Within 3 hrs	Upon request	24 clock hours or less	80% rising to 85% within first 6 months of rollout; Reassess target at end of 6 months
4	1 business day	Within 1 business day	Upon request	3 business days	80% rising to 85% within first 6 months of rollout; Reassess target at end of 6 months
5	1 business day to acknowledge receipt of request / order	SLA or as agreed upon with Customer	Upon request	SLA or as agreed upon with Customer	SLA or as agreed upon with Customer

2.10 Customer Notification

ITS will provide all communications via the following means: online ticket updates, phone calls, and/or email notifications utilizing the customer contact information (see Customer Responsibilities).

2.11 Customer Escalation Contact List

The ITS Customer Support Center is the Single point of contact for all incidents to be reported to ITS. Please contact the ITS Customer Support Center (CSC) at **919-754-6000** or toll free at **1-**

800-722-3946 to report any incidents or to initiate service requests. Contact may also be made by emailing the CSC at ITS.Incidents@ncmail.net.

If there is reason to believe that the incident or request is not being handled appropriately or if additional questions need to be answered about ITS services, their business value or ITS Processes, contact the Business Relationship Manager assigned to your agency

If this does not satisfactorily resolve the issue please contact the Director of Business Relationship Management, Wendy Kuhn. Subsequent escalations, where necessary should be to Deputy State CIO, Bill Willis and then State CIO, George Bakolia

At any time the Business Relationship Manager can be called to help explain ITS services or work with the business team on information technology business needs.

3 Customer Responsibilities

ITS and the Agency will work together to make sure that all responsibilities can be met. Below are responsibilities for which ITS will need support and ownership from the Agency:

- Provide advance requirement documents that define customer hosting and storage requirements and design to support new hardware and client application requirements
- Provide utilization estimates or anticipated changes in application requirements that are needed to assess future capacity needs
- Request and schedule special services (for example, installation of new equipment, after-hours support) well in advance
- Application or database changes that have the potential to result in enterprise wide impacts must go through the ITS Change Management process.
- Customer agrees to establish a point of contact (POC) for ITS to contact for reporting and coordinating outages or emergency maintenance
- Customer agrees to use the ITS Customer Support Center for reporting incidents or requesting assistance
- Customer shall use the service for lawful purposes only and comply to ITS and State CIO Security Standards and Policies
- Customer agrees not to tamper with ITS equipment, including access of configuration files or physically altering the equipment
- Customer agrees to work with ITS on a mutually agreed schedule to allow required maintenance services to be performed in a timely manner

4 Performance and Service Level Reviews

A basic goal of ITS management is to keep the customer regularly informed. Status meetings, status reports, performance measurements, and planning sessions are the vehicles used to

ensure that the Customer is kept apprised of activities. ITS management believes that to provide effective services to the customers, management must maintain awareness of events and make effective use of all resources. This will position ITS to meet the service level commitment to our customers.

Monthly - There will be a monthly meeting with the Agency and the Business Relationship Manager from ITS providing a scorecard to the agency of the performance of ITS services.

Semi-Annually (or as needed) – There will be a semi-annual performance review with the Agency, State CIO and Business Relationship Manager from ITS. This discussion will provide information on performance by ITS in providing the service outlined in this SLA. This will also be used to make ITS aware of business events or changes that may impact or change the services provided by ITS.

Yearly – There will be a yearly service review meeting to provide metrics and measurement to determine if the service level requirements have been met for the agency. If requirements are not met or partially met then improvement areas will be developed with action plans for changes to improve the service.

The SLA will also require review under any of the following conditions:
1) Whenever there is a significant and/or sustained change to the delivery of the Hosting Services
2) Whenever there is a significant and/or sustained change requested to the SLA that supports the Hosting Services

Performance and Availability

Services will be available 24 x 7 x 365 days a year excluding scheduled outages. All problem tickets will be entered and tracked using the Customer Support Center system. All problems encountered will follow the production escalation process.

Performance and Availability	
Availability	The environment will be available based on a 24 x 7 x 365 schedule (excluding scheduled outages) as measured on a one (1) month interval. ITS Hosting Services will provide the designated Customer representative with a periodic planned maintenance schedule.
Operational Reporting	ITS Hosting Services will provide mutually agreeable environment diagnosis tools that will facilitate the identification of any disruptions/bottlenecks in service that occur in the service delivery of the Customer solution. This diagnosis is limited to network segments and components controlled by the ITS Hosting Services.
Scheduled Downtime Change	Three levels are used to describe the Request for change: • **Major** – (20 Business days Lead Time) If the Request for Change (RFC) will (or could have) Global impact and/or substantial financial, ITS resource commitment, or client impact, it is identified as a Major Change. All Major Changes require senior management endorsement prior to

Performance and Availability	
	Change Advisory Board review • **Significant** – (10 Business days Lead Time) If the Request for Change (RFC) will (or could have) localized and substantial, financial, ITS resource commitment of client impact it is identified as a Significant change. Significant changes require Change Advisory Board (CAB) review. • **Minor** – (3 Business Days Lead Time) The change has little or no impact, but is not a pre-approved event, it can be authorized by the Change Manager
Contingency Downtime	ITS Hosting Services reserves the authority to take down any system to perform maintenance in the event of an emergency (e.g. hacked server, emergency patch requirements). ITS Hosting Services will make every effort to inform customer and feedback ongoing status.
Hardware Monitoring	Monitored 24 x 7 x 365 days a year.
System Resource and Utilization Monitoring	Monitored 24 x 7 x 365 days a year.
Operating System Monitoring	Monitored 24 x 7 x 365 days a year.
Network Monitoring	Monitored 24 x 7 x 365 days a year.
Emergency OS Patches	As required.
Emergency Security Patches	As required.
State declared emergencies	To be performed in accordance with the Disaster Recovery Plan.
Disaster Recovery	Disaster Recovery will only be provided for those applications specified to require disaster recovery.

5 Change Control

Customer will appoint a primary and an alternate Point of Contact (POC) to serve as a liaison with the ITS. These POC's will be responsible for all technical communications, approvals, and change requests initiated by the Customer. ITS will only contact the alternate POC(s) if the Primary POC is not available. The POC should be established as an escalation list (up to 3 individuals), with appropriate contact alternatives to allow a timely response in case of an emergency. Customer's POC will report any change requests to the Customer Support Center (CSC), and request a ticket to be opened, indicating the nature of the request (emergency or planned). ITS will handle configuration change requests according to one of the following categories:

Planned changes – implemented during scheduled maintenance windows. Three levels are used to describe the Request for change:

a. **Major** – (20 Business days Lead Time) If the Request for Change (RFC) will (or could have) Global impact and/or substantial financial, ITS resource commitment, or client impact, it is identified as a Major Change. All Major Changes require senior management endorsement prior to Change Advisory Board review
b. **Significant** – (10 Business days Lead Time) If the Request for Change (RFC) will (or could have) localized and substantial, financial, ITS resource commitment of client impact it is identified as a Significant change. Significant changes require Change Advisory Board (CAB) review.
c. **Minor** – (3 Business Days Lead Time) The change has little or no impact, but is not a pre-approved event, it can be authorized by the Change Manager

Emergency changes – 4-hour response, 24 x7 x 365.

6 Security Standards and Policies

This SLA is in compliance with ITS and State CIO Security Standards and Policies.

7 Business Continuity Plan

This SLA is supported by a Business Continuity Plan as specified in ITS ISO Business Continuity Plan. Agency responsibilities should be documented in a corresponding agency business continuity plan.

8 Dispute Resolution for Service Impacting Outages or Failure to Perform

ITS and the agency agree that it is in their mutual interest to resolve disputes informally. When there is a dispute about a "service impacting outage" or a failure in performance occurs, the Agency Secretary or Agency Deputy Secretary shall contact the State Chief Information Office (CIO). A report shall be prepared that identifies the underlying cause and a remediation action plan shall be developed and agreed upon by both agencies. The State CIO and Agency Secretary or Agency Deputy Secretary shall meet and discuss any changes needed to be made by either ITS and/or the agency. If the agency is not satisfied with the resolution, the agency may refer the matter to the Office of State Budget and Management for its review and recommendation.

9 Metrics and Reports

Report name	Reporting Metric	Reporting interval	Reporting Source	Delivery method
Incident and Request Time to Repair Analysis	Percentage of requests and incidents resolved within target timeframe, minus lost time	Monthly	iWise	Email
Incident and Request Resolution Performance	Mean time to Repair - MTTR minus lost time resolved within target time frame	Monthly	iWise	Email

Archival of all reports shall follow the records retention schedule adopted by the North Carolina Office of Information Technology Services and the State Records Branch General Schedule, as applicable.

10 Definitions

Terminology	Description
Application	Generic term for a program, or system that handles a specific business function.
Application Software	A complete, self-contained program that can perform work for a user. This is in contrast to system software such as an operating system and server processes that exist in support of application software.
Backup and Recovery	Backup is the process of ensuring that a copy of the data is available to be used in the event that the original material is no longer available.
BMC Patrol	Tool installed on equipment to help monitor trouble event and send alerts in the form of pages or emails to technical support people.
Business Continuity	Business Continuity is the process of ensuring that essential functions are in place and available so that an organization can survive and continue to operate when an emergency occurs. One of these functions might be information technology, another might be facilities management or accounting. It depends on the organization's mission.
Change Management	Process that is responsible for controlling change to all technology components within a production or test environment.
Computing Services	Division within ITS that handles all servers, middleware, storage, backup, large printing, as well as the operational and support personnel to run the IT technology.
Configuration Management	Recording and documenting the components that make up a server solution for a business application. Includes both hardware and software components.
Business Relationship Manager	Position in ITS that works the senior management of an agency to help provide understanding and foster business relationships between ITS and the agency.
Customer Support Center	Central team that is the single point of contact for agency customers to report problems or request services from ITS.
Disaster Recovery	Disaster Recovery is the process of ensuring that the information technology and other needed infrastructure is recovered and in a condition to support the organization's survival in an emergency.
Emergency Maintenance Windows	A timeframe where IT infrastructure will be taken out of service to fix a problem that is outside of the normally scheduled maintenance timeframe.
Hosting	Providing hardware, software and services to allow business applications to run on a server or set of servers.
Incidents	A failure in hardware, software or services that results in a customer not being able to utilize technology.
Internet Network Components	Infrastructure that is outside of ITS supported equipment that is needed to support Wide Area Network services. Examples may be POP site equipment or Telco Central Office equipment.
Internet Protocol (IP)	An identification method to give each device on a network a number/name so that information is appropriately distributed.
iWise	ITS IT Service Management tool used to track work within ITS including incidents, problems, requests, and changes.
Local Area	A computer network that spans a relatively small area. Most LANs are confined

Network	to a single building or group of buildings.
Mean Time To Repair (MTTR)	The average amount of time, typically in minutes it takes to restore/repair service. This includes prime time and weekend and holiday guarantees.
Operating System (OS)	System software that controls data storage, input and output to and from the keyboard, and the execution of applications written for it. It performs base services: prioritizing work, scheduling, memory management, etc.
OS Patch	As the OS vendor resolved known defects or makes improvements to the OS, the OS patches are sent to ITS to resolve or prevent potential issues that could be catastrophic.
Patch	Code or configuration fix received from a vendor that needs to be applied to prevent failures.
Point of Contact	Person within an agency that is responsible for working with the Local Area Network team to schedule changes or maintenance windows needed for infrastructure improvements or repair.
Server	A computer on a network that makes applications, print services, data, and communications available.
Schedule Maintenance Windows	A timeframe where IT infrastructure is taken out of service for maintenance. This is done with knowledge and approval from the customer.
Telecommunication Services	Organization within ITS that supports the local area network, wide area network and voice services.
Utility Support Software	Software that is needed to run and maintain a server outside of the vendor operating system. This may include backup software, monitoring software and other services.

11 Signatures of Approval

Agency Secretary or Deputy Secretary:

Name	Title	Signature	Date

ITS Senior Management**:**

Name	Title	Signature	Date

Appendix A: Supported Hardware and Software

Supported hardware

ITS will use standard hardware environments to service customer hosting solutions based on guidelines and requirements needed to support customer requirements

Customer provided hardware may be used to host the customer's application to transition to ITS provided hardware when transitioning during consolidation efforts, migration from remote to central site, and to transition from customer to ITS management.

Hardware services

The following hardware services are provided:

- Recommendations: ITS is responsible for assisting in specification and recommendation of hardware solutions
- Design and Configuration: ITS is responsible for assisting clients with solutions that meet their server requirements.
- Diagnosis: ITS will perform 1st and 2nd level hardware problem determination for the server infrastructure.
- Installation - ITS will install, configure and customize hardware and operating systems.
- Maintenance - ITS will maintain hardware and operating systems by direct service or through contracted vendor support. This includes maintaining a quarterly schedule for operating systems patching, and hardware firmware updates.
- Connectivity: ITS is responsible for coordinating the successful connection of the server to it's SAN and to the appropriate network
- Upgrades - ITS will assess, upgrade, or add components to meet customer requirements
- Monitoring / Alerting – ITS will establish standard hardware and resource utilization criteria to ensure hardware health.
- Capacity Management – ITS will analyze hardware hosting to ensure there is sufficient resources to support the hosted applications processing and storage demands.
- Repair – ITS will repair or dispatch repair of hardware (dispatch and completion of work estimates will be according to service type selected by the customer)
- Backup/Restore - ITS will provide backup and restore services for customer data server per the established specifications.
- Disaster Recovery - hardware recovery and restoration of customer data is optional and will be done per the established specifications

Unsupported hardware

The following are representative, but not comprehensive, examples of hardware that is *not* supported:

- Hardware solutions that are not contracted for ITS support
- Customer provided and supported hardware

Software Services

The following software services are provided:

- Recommendations: ITS is responsible for assisting in the evaluation and recommendation of Operating systems and associated upgrades
- Diagnosis:
    - ITS will perform 1st and 2nd level software problem determination and resolution for the server infrastructure

    - ITS will not perform problem determination and resolution for application software
- Installation and configuration: ITS is responsible for the installation of server operating systems and for configuring software for the server per the established specifications
- ITS is responsible for evaluating and recommendation of software on a per case basis

Supported software

The following operating systems software is supported:

- AIX 5.1
- Solaris 9 & 10
- Red Hat Linux AS, ES 3.1 & 4.0
- Windows 2003, 2000
- Netware 5.1 & 6.5

Unsupported software

The following software is *not* supported:

- Operating systems not listed above
- System software not recommended or approved by ITS
- Application software

Appendix B: Hosting Services Special Amendments

1. System Backup and System Recovery

a. Backup Tool

NetBackup Server software is the ITS' backup and recovery solution designed for use with a myriad of configurations to include the customer's hosted environment. It enhances speed of recovery, performs sophisticated backups that limit the impact on applications and host, and allows for automated disaster recovery. It provides media management features that address tape duplication to library and drive sharing.

b. Recovery Time Objective

Recovery Time Objective	
Operating Systems	Best effort
File Systems	Best effort

c. Recovery Point Objective

Recovery Point Objective	
Operating Systems	ITS' objective is last known full backup or last known incremental backup.
File Systems	ITS' objective is last known full backup or last known incremental backup.

d. Backup Schedule and Retention

Backup, Restore and Recovery Schedule	
Backup and Retention	ITS is responsible for file level system backups and shall supply the hardware and software necessary. These backups are included in the basic monthly fee for service described in this SLA. • Incremental backups will be performed daily and those tapes will be kept on-site for 14 days. Backups will be removed to on-site storage immediately after creation and kept in ITS' silo. • One full backup will be done weekly. One backup will be kept off-site for one month. One backup will be kept in ITS' silo for 14 days. • Backups going to the off-site facility will be sent on ITS' schedule per the storage facility. • Off-site storage will be in an industry approved data protection facility designated by ITS.
Restore	ITS will coordinate any software and hardware repairs and restore, as applicable, operating environment and

	file systems containing the Customer's application data from the latest backup.

2. OS – Operating System

ITS will be responsible for maintaining server operating system (OS) level software. A minimum of N-1 level of OS maintenance will be sustained as defined by the ITS. ITS commits to providing all OS service packs on the server configuration as needed. For problems encountered that can be remedied by a specific patch, the patch will be provided.

ITS will work with the customer to coordinate OS plans. Such coordination may result in deferred patch application, in order to minimize user impact and align patch operations with scheduled maintenance periods.

ITS will maintain Change Management and server configuration management over all components of this service. The Customer will be responsible for administrative support such as account creation, group creation, rights assignments, application installation, and password administration. The Customer will follow all ITS Change Management procedures.

ITS will assign server names and volume names in accordance with statewide naming standards.

Any major OS version upgrades (for example: version 1.x to version 2.x) requested by the Customer will be considered a separate project that will be billed on a time and materials basis. The customer will be billed when the upgrade results in a new version of an OS that is not yet supported by ITS. Supported OS upgrades will be at no charge.

3. OS Patches

ITS in accordance with standard procedures will apply OS patches to the hosted environment.

ITS will notify Customer when OS patches become available. In accordance with a coordinated maintenance schedule, ITS will install OS patches. ITS is responsible for applying appropriate aspects of the statewide Vulnerability Management Standard when considering and implementing OS patches. Of equal concern is the stable operation of the Customer application, which is complex and which may be destabilized without proper configuration management

The Customer is responsible for working with application vendors or developers to determine compatibility with proposed upgrades. In the event that the Customer is aware of a known conflict between the hosted applications and the proposed patch, update, or service pack, the customer may elect to defer the upgrade. However, deferring ITS' recommended upgrades might impact server reliability. The Customer will assume all risks and take responsibility for any adverse performance or availability to the OS for the hosted environment.

The Customer's CIO/CTO, may deny such permission by providing a written explanation to the Customer Support Center that addresses their security needs and how ITS' action would not be beneficial, necessary or proper. The Customer will provide a mitigation plan and timing of when with OS patch should be installed. The mitigation plan will also include any known future OS patches and the order of implementation.

ITS acknowledges that vendor and/ or developer inquiry into the effects of upgrade or patch revision often requires a two-week turnaround period.

ITS will notify customer of:

- The patch that needs to be applied
- Proposed installation date which will be based on the change management process and submitting a request for change, see section 5.0. Where feasible, installation date will be based on coordinated maintenance schedule.
- The outage duration needed to apply the patch
- ITS will perform system upgrades during the maintenance window of 4:00 a.m. to 12:00 noon on Sundays. Other maintenance can be scheduled outside of the maintenance window based on urgent or emergency change needs.

4. Security Patches

ITS will take virus protection measures and other security precautions in accordance with ISO standards and the state's Vulnerability Management Standard in applying security patches to the hosted environment.

ITS will notify Customer of:

- The security patch that needs to be applied
- Proposed installation date which will be based on the change management process and submitting a request for change, see section 5.0. Where feasible, installation date will be based on coordinated maintenance schedule.
- If a high security situation creates significant vulnerability, ITS will follow the emergency Change Management procedures to implement those fixes.
- The outage duration needed to apply the security patch
- Any virus detections or intrusions

In the event that the Customer is aware of a known conflict between the hosted applications and the proposed security patch, the customer may elect to defer the patch. The Customer will assume all risks associated with not installing the patch.

The Customer's CIO / CTO, may deny such permission by providing a written explanation to the Customer Support Center that addresses their security needs and how ITS' action would not be beneficial, necessary or proper. The Customer will provide a mitigation plan and timing of when the security patch should be installed.

Security patches are of great concern and pose vulnerability threats. As new intruders are detected, it is of extreme importance that ITS be allowed to be proactive to protect confidential student data. Of equal concern is the stable operation of the Customer application, which is complex and which may be destabilized without proper configuration management.

5. Change Management Process

Three levels of Type are used to describe the Request for change:

Major – (20 Business days Lead Time) If the Request for Change (RFC) will (or could have) Global impact and/or substantial financial, ITS resource commitment, or client impact, it is identified as a Major Change. All Major Changes require senior management endorsement prior to Change Advisory Board review

Significant – (10 Business days Lead Time) If the Request for Change (RFC) will (or could have) localized and substantial, financial, ITS resource commitment of client impact it is identified as a Significant change. Significant changes require Change Advisory Board (CAB) review.

Minor – (3 Business Days Lead Time) The change has little or no impact, but is not a pre-approved event, it can be authorized by the Change Manager

Appendix C: Application Requirements and Special SLA needs